Amendments to the Claims

1. (Currently amended) Method of securing messages exchanged over a data transmission network between a server (1) and a small client (2) that does not have the resources necessary for providing security functions, under the control of an authority that defines message exchange rules, ~~characterized in that~~ wherein control is provided in a decentralized manner by a representative (3) of the authority, inserted permanently into the network in the vicinity of the client (2) and between the server (1) and the client (2) during the secure exchange of messages, to translate transmitted messages and to apply verifications decided on by the authority to transmitted messages.

2. (Currently amended) Method according to claim 1, ~~characterized in that~~ wherein a first protocol (P) is used for exchanges between the server (1) and the representative (3) of the authority, and a second protocol (P') different from the first protocol (P) is used for exchanges between the representative (3) of the authority and the client (2).

3. (Currently amended) Method according to claim 1, ~~or claim 2,~~ ~~characterized in that~~ wherein, for the exchange of messages:

a first secure channel (4) is set up between the server (1) and the representative (3) of the authority, using a first key (Ks) known to the representative (3) of the authority and to the server (1) but not to the client (2), and using a first encryption algorithm (AL), and

a second secure channel (5) is set up between the representative (3) of the authority and the client (2), using a second key (Kc) known to the

representative (3) of the authority and to the client (2) but not to the server (1), and using a second encryption algorithm (AL').

4.   (Currently amended) Device for securing messages exchanged over a data transmission network between a server (1) and a small client (2) that does not have the resources necessary for providing the security function, under the control of an authority that defines message exchange rules, ~~characterized in that it comprises~~ comprising a decentralized control device or representative (3) of the authority, inserted permanently into the network in the vicinity of the client (2) and between the server (1) and the client (2) during the secure exchange of messages, to translate transmitted messages, and to apply verifications decided on by the authority to transmitted messages.

5.   (Currently amended) Device according to claim 4, ~~characterized in that~~ wherein the decentralized control device or representative (3) of the authority is a data processing microsystem secured by hardware, inserted permanently between the server (1) and the client (2) during the exchange of messages.

6.   (Currently amended) Device according to claim 5, ~~characterized in that~~ wherein:
    the server (1) is a data processing system comprising an input-output port (1a);
    the client (2) is a data processing microsystem comprising an input-output port (12);
    the representative (3) of the authority is a data processing microsystem secured by hardware and comprising an interface device (13);

3

a dedicated interface system (7) is provided, comprising an input-output port (8) connected to the input-output port (1a) of the server data processing system (1), comprising a card port (9) connected to the input-output port (12) of the client data processing microsystem (2), comprising an input-output port (10) connected to the interface device (13) of the representative (3) of the authority data processing microsystem, and comprising a controller (11) programmed to control communication between the input-output ports (8), (9) and (10);

the controller (11) and the representative (3) of the authority are programmed so that:

the server data processing system (1) sends a request A to the client data processing microsystem (2), and that request is received by the controller (11);

the controller (11) transmits the request A to the representative (3) of the authority, which sends it back a response Ra;

the controller (11) uses that response Ra to calculate a request A' that is sent to the client data processing microsystem (2);

the client data processing microsystem (2) processes the request A' to prepare a response B';

the client data processing microsystem (2) sends the response B' to the server data processing system (1); that response is received by the controller (11);

the controller (11) transmits the response B' to the representative (3) of the authority, which sends it back a response Rb;

the controller (11) uses that response Rb to calculate a response B that is sent to the server data processing system (1).

7. (Currently amended) Device according to claim 6, ~~characterized in that~~ wherein:

the client (2) is a smart card;

the representative (3) of the authority is a smart card;

the dedicated interface system is a smart card reader (7) comprising two card ports (9) and (10).

8. (Currently amended) Device according to claim 6, ~~characterized in that~~ wherein:

the client (2) is a mobile communication system;

the server (1) is a data processing system communicating with the client (2) via a physical connection or via a wireless communication network;

the representative (3) of the authority is a smart card representing the operator of the wireless communication network (known as the SIM card in telephones conforming to the GSM standard).

9. (Currently amended) Device according to claim 6, ~~characterized in that~~ wherein:

the client (2) is a smart card;

the representative (3) of the authority is a data processing system secured by hardware;

the dedicated interface system (7) is a machine comprising a card port (9) and a dedicated input-output interface (10) for connection to the representative (3) of the authority data processing system.